NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

THE ENCRYPTION EXPORT POLICY CONTROVERSY: SEARCHING FOR BALANCE IN THE INFORMATION AGE

LT COL MARCUS S. MILLER/CLASS OF 2000
COURSE 5603
SEMINAR F

FACULTY SEMINAR LEADER:
AMB ROBERT PRINGLE

FACULTY ADVISOR:
COL JACK E. LEONARD

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2000	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Encryption Export Policy Controversy: Searching For Balance in the Information Age	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University National War College Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**24**	

THE ENCRYPTION EXPORT POLICY CONTROVERSY: SEARCHING FOR BALANCE IN THE INFORMATION AGE

> …information is the most valuable commodity. The exchange of digital information has become an integral part of our society….(and) the success of the Information Age depends on the ability to protect information as it flows around the world, and this relies on the power of cryptography. Encryption can be seen as providing the locks and keys of the Information Age.[1]

INTRODUCTION

The Information Age challenges old paradigms and severely tests the government's ability to devise appropriate and effective national policies. The federal government's encryption export policy highlights a complex information age issue involving seemingly insurmountable conflicts between national security, law enforcement, privacy, and business interests. Encryption employs mathematical algorithms, implemented in either hardware or software, to encode or scramble a sequence of data. Although cryptography has been used for centuries, the rise of the Internet and electronic commerce pushed the issue of encryption control to the forefront of public debate during the 1990s. Formerly the near-exclusive domain of governments, the majority of today's encryption products flow from private industry backed by private funding for use in the private sector.[2] While encryption rose to increasing importance in cyberspace to secure communications and establish trustworthiness, the federal government continued to follow the traditional national security paradigm of export controls. A series of policy decisions by the Clinton Administration on encryption export controls during the 1990s ignited a heated public discourse and a continuing search for a balance between competing interests. The

---

[1] Simon Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (New York: Doubleday, 1999), 293.

[2] *Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo* by William H. Webster, chairman, Global Organized Crime Project (Washington D.C.: Center for Strategic and International Studies, 1998), 60.

Administration's pursuit of balance apparently reached its end-state with an announcement on September 16, 1999 to reverse US export restrictions on strong encryption, a radical departure from previous reliance on export controls.[3] The federal government's search for balance among competing interests in its encryption export policy illustrates the substantial difficulties facing policy makers in the Information Age. While the search for policy balance appears to prove the ultimate adequacy of the Constitutional framework and the policy making process to deal with complex issues in cyberspace, it clearly highlights the imperative for national policy makers to recognize Information Age realities, the inherent limitations of government policy in this arena, and the process shortcomings that obscure and obfuscate Information Age truths.

COMPETING INTERESTS

> Encryption is the Bosnia of telecommunications policy…stakeholders take positions that polarize rather than reconcile.[4]

The encryption export policy debate generates vigorous arguments by various actors and communities representing both sides of the issue. Achieving policy balance on this issue confronts a fundamental tension between two competing objectives: (1) making encryption widely available so that individuals, businesses, and organizations can protect themselves, and (2) restricting the proliferation of strong encryption to prevent its use by hostile foreign powers, terrorists, and criminals.[5]

---

[3] The White House, Office of Press Secretary, *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace*, William Cohen, Janet Reno, Jacob J. Lew, and William Daley, September 16, 1999, 5; available at <http://www.epic.org/crypto/legislation/cesa/report_9_16_.html>; accessed on November 8, 1999.

[4] Kenneth W. Dam and Herbert S. Lin, "Protecting Information in Cyberspace," National Academy Op-Ed Service, September 13, 1966; available at <http://www4.national academies.org>; accessed on December 7, 1999.

[5] Joan D. Winston, Kenneth A. Mendelson, and Stephen T. Walker, "Light at the End of the Tunnel? Finding a Way Through the Crypto Policy Impasse" (151-165) in *Cyberwar 2.0: Myths, Mysteries and Reality* eds Alan D. Campen and Douglas H. Dearth (Fairfax: AFCEA International Press, 1998), 152.

In pursuing controls on encryption techniques, the federal government sought to restrict foreign use of strong encryption and, secondarily, to ensure a means for law enforcement access to communications and computer data. "As increasingly sophisticated and secure encryption methods are developed, the government's interest in halting or slowing the proliferation of such methods has grown keen."[6] The national security establishment began to lose control of encryption technology during the 1970s with the development of public key systems outside the domain of the National Security Agency (NSA), the Department of Defense agency tasked with signals intelligence. National intelligence agencies feared that widespread proliferation of strong encryption would make it harder to intercept, analyze, and exploit communications of foreign governments and other adversaries in a timely fashion, thus compromising a vital intelligence capability that contributes substantially to national security.[7]

US law enforcement, spearheaded by the Federal Bureau of Investigation (FBI), worried that the use of strong encryption by criminals and terrorists negates the utility of wire-tapping, an invaluable investigative technique. The law enforcement community "argued that effective wire-tapping is necessary in order to maintain law and order, and that encryption should be restricted so that they can continue with their interceptions."[8] The FBI believed that unbreakable encryption shifts the long-standing balance between law enforcement and individual privacy inappropriately towards privacy. Thus, in addition to supporting export controls, the FBI showed an equal interest in promoting key

---

[6] United States Court of Appeals for the Ninth Circuit, *Bernstein vs US Department of Justice*, Case Number: 97-16686, filed May 6, 1999, 6; available at <http://www.epic.org/crypto/export_controls/bernstein_decision_9_cir.html>; accessed on November 27, 1999.

[7] Barbara McNamara, Testimony before the U.S. House of Representatives Judiciary subcommittee, March 4, 1999; available at <http://www.usia.gov/current/news/latest/99030402.clt.html?/products/washfile/newsitem.shtml>. U.S. Court of Appeals for the Ninth Circuit, *Bernstein vs US Department of Justice*, 6.

[8] Singh, *The Code Book,* 304.

recovery systems (also called key escrow or key management) where a trusted third party holds and safeguards encryption keys to enable rapid access for law enforcement under court authorizations. The FBI had even proposed incorporating a trapdoor design in all encryption products to allow secretive government access.[9]

Countering the national security and law enforcement communities, the private sector voices an equally strong opposition to restrictions on the free development, use, exchange, and export of encryption for a variety of reasons, ranging from the right to privacy to the need to promote electronic commerce. Considering privacy as a fundamental human right, civil libertarians invoke the Fourth Amendment in support of their claims and view "the widespread use of encryption as essential for guaranteeing the right to privacy."[10] The concerns shaping the outlook of privacy advocates include the progressive erosion of individual privacy in the Information Age, the grave potential for misuse of sensitive personal data, and an underlying mistrust of the "motives and methods of federal government agencies."[11] Civil libertarians remain especially frightened with the federal government's aggressive promotion of key recovery, since it creates an infrastructure that facilitates social control by government and exacerbates the potential for privacy invasion by overzealous authorities.[12]

The business community's interests obviously lie in maintaining strength and profitability of the high-tech industry while advancing the vast promise of commerce in cyberspace. US businesses argued that export restrictions undermine the competitive

---

[9] Solveig Singleton, *Encryption Policy for the 21st Century: A Future Without Government-Prescribed Key Recovery*, Cato Institute Policy Analysis No. 325, 2. *Cybercrime, Cyberterrorism, and Cyberwarfare*, 60.
[10] Singh, *The Code Book*, 306.
[11] *Cybercrime, Cyberterrorism, and Cyberwarfare*, 60-61.
[12] Singh, *The Code Book*, 310-313. Singleton, *Encryption Policy for the 21st Century*, 30-31, 37.

edge of US computer, software, and telecommunications industries in an increasingly global marketplace. Additionally, business views the widespread use of strong encryption, both domestically and internationally, as crucial to establishing a level of trust in cyberspace that will fully promote the growth of electronic commerce.[13]

BELATED RECOGNITION OF POLICY IMBALANCE

> Sometime during the last decade, for both technological and economic reasons, that regulatory balance point, heavily weighted on the side of national security, became both obsolete and inappropriate. During the 1990s we have seen the mismatch between encryption export controls and the realities of the global marketplace become more and more painful to industries and consumers and, no doubt, to the regulators themselves.[14]

The Clinton Administration long sought to find a balance in US encryption policy and consistently articulated balance as its chief policy objective. However, it faced an increasingly difficult task in attaining this objective given an increasing need for strong encryption to support electronic commerce combined with the greater sophistication of foreign encryption products and an expanding group of international software vendors.[15] In a series of proposals during the 1990s, the Administration's policy incrementally shifted in favor of relaxation, yet each change in policy failed to attain a balance and faced stiff resistance from the private sector and Congress (see Table 1). The September 16, 1999 proposal, the latest in a series of formal policy announcements on encryption controls since 1993, may finally achieve the desired balance among competing interests. By effectively halting export controls on encryption of any key length (an approximation of the relative strength of a particular code), this policy represents a radical departure from previous approaches. The incremental changes reflected a growing realization by

---

[13] Kenneth N. Cukier, "Scrambled Codes," *Red Herring* (December 1999), 227-228.
[14] Winston, et al., "Light at the End of the Tunnel?," 152.
[15] The White House, *Preserving America's Privacy and Security in the Next Century*, 5.

policy makers of the limitations and ultimate outcomes of encryption export controls—global proliferation of strong encryption was an inevitable, yet necessary evil.

TABLE 1. SUMMARY OF CLINTON ADMINISTRATION PROPOSALS ON ENCRYPTION EXPORT CONTROLS

PROPOSAL	KEY FEATURES
Clipper Chip (April 1993)	- Designated Clipper Chip as federal government encryption standard - Government designed algorithm with key information kept in escrow with Dept of Commerce and Dept of Treasury - No export controls on Clipper encryption
Clipper II (1995)	- Allowed export relief for commercial key escrow systems - Government certified trusted third party would hold copies of all keys - Government could access through court orders
Clipper III (Summer 1996)	- Established key management infrastructure with trusted certification authorities - Exports permitted as long as keys held in escrow with certification authorities
Clipper Chip 3.1.1, Executive Order 13026 (November 1996)	- Transferred responsibility for export controls from State Department to Commerce Department - 56-bit encryption permitted for export by companies that make commitments to develop and market key recovery - Special envoy appointed to promote international cooperation on encryption
Limited relief of encryption export controls (September 1998)	- Decontrols 56-bit encryption products after one time technical review - Allows increased bit-length products for specialized industry groups and on-line merchants - Unlimited key length exports permitted to US subsidiaries - Export of strong encryption permitted for key recovery systems - Promised new solution by December 15, 1999
Broad relief of export restrictions and a new legislative proposal on law enforcement access, Cyberspace Electronic Security Act (CESA) of 1999 (September 16, 1999)	- Allows export of any encryption product of any key length - One time technical review of products prior to export - Precludes encryption exports to states supporting terrorism - Post export reporting - Sets standards for law enforcement access to keys held by trusted third parties - Protects law enforcement sources and methods from court disclosure

Sources:

1. Center for Democracy and Technology, "An Overview of Clinton Administration Encryption Policy Initiatives," available at <http://www.cdt.org/>.
2. Solveig Singleton, *Encryption Policy for the 21st Century: A Future Without Government Prescribed Key Recovery*, Cato Institute Policy Analysis No 325, November 19, 1998.
3. The White House, Office of Press Secretary, *FACT SHEET: Administration Updates Encryption Export Policy*, September 16, 1999.
4. Kenneth N. Cukier, "Scrambled Codes," *Red Herring* (December 1999), 230.

The federal government eventually understood the global dynamics of the information technology industry and marketplace would prevent export restrictions from effectively controlling the proliferation of encryption technology. "In a global market in which the capabilities of the developing countries are steadily improving and trade

barriers are falling, the ability of government to restrict technologies is extraordinarily limited."[16] In general, export controls make a net difference only when the US is the sole source of information about a technology or when other similarly capable countries also maintain export controls. Many foreign governments refused to adopt encryption export controls, and thus offered safe havens for the manufacture, use, and distribution of encryption. Additionally, strong encryption code developed in the US can easily be smuggled abroad, physically or virtually.[17] Heavy-handed government efforts to promote escrowed encryption also failed to attract sufficient end user interest or establish the commercial viability of widespread key recovery.[18]

The Clinton Administration also came to realize the counterproductive side effects of export restrictions. Export controls tended to be de facto domestic controls and thus reduced the availability and use of strong encryption for domestic applications.[19] By inducing uncertainty over government policies that complicated planning by industry and end users, the public controversy and incremental policy changes surrounding export controls and key recovery inhibited the widespread employment of encryption. "Vendors are reluctant to bring to market products that support security, and potential users are reluctant to adopt information security products that may become obsolete if and when the legal and regulatory environment changes."[20] The government also understood export restrictions pushes foreign consumers away from US products, and in effect, subsidizes foreign production of encryption products. Export controls on encryption placed US

---

[16] *Cybercrime, Cyberterrorism, and Cyberwarfare*, 58.
[17] Singleton, *Encryption Policy for the 21st Century*, 18.
[18] Winston, et al., "Light at the End of the Tunnel?," 163.
[19] Ibid, 163.
[20] Fred B. Schneider, ed., *Trust in Cyberspace* (Washington D.C.: National Academy Press, 1999) 211-214.

businesses at a disadvantage in global markets, undermined US competitive edge in information technology, and allowed the emergence of a robust encryption sector outside the US. "Hobbled by a convoluted, confusing, and time-consuming export-licensing regime, many American firms lost big sales outside the United States to the emerging European players." Estimates of US industry losses for 1998 and 1999 in forgone software sales and indirect productivity benefits range from $4.2 billion to $16.6 billion and projection of loses through 2004 range between $37 billion and $96 billion.[21]

More importantly, the Clinton Administration grasped the larger national security and economic implications of its policies. Reduced export controls would promote the use and standardization of encryption and thus promote information system security, trustworthiness in electronic commerce, and protection of critical cyber-based national infrastructures.[22] The Administration conceded encryption had emerged as a vital component of the global information infrastructure and digital economy because it was essential to provide security, integrity, and privacy for interactions in cyberspace, especially electronic forms of business and commerce. "Without the use of encryption, it is difficult to establish the trust that people and firms need to do business with each other, or to have confidence to run their business electronically."[23]

THE POLICY PROCESS AT WORK

The Clinton Administration's spin on its latest proposal suggests that the outcome demonstrated a government process that succeeded in finding a balance. The people and government worked together in pursuit of a common objective: "to provide the tools to

---

[21] Cukier, "Scrambled Codes," 228-232. Arnold G. Reinhold, *Strong Cryptography: The Global Tide of Change*, Cato Institute Briefing Paper No. 51, September 17, 1999, 3; available at <http://www.cato.org>.
[22] Singleton, *Encryption Policy for the 21st Century*, 21. Schneider, *Trust in Cyberspace*, 214.
[23] The White House, *Preserving America's Privacy and Security in the Next Century*, 4.

keep our nation safe, while taking technological advances and market changes into account."[24] Such a statement, especially coming at the end of a long and arduous process begs several questions: What did balance mean to the Clinton Administration? How was balance sought? While full answers may have to wait for the dust to settle and the arrival of the next administration, one can at least surmise a partial answer.

Applying the models of public decision making yields some clues to the meaning and practice of balance. In the organizational behavior model Allison and Zelikow claim that the actions of government can often be understood "...less as deliberate choices and more as outputs of large organizations functioning according to standard patterns of behavior."[25] Organizations focus on unique problems that define their mission and develop special capacities to aid in mission accomplishment.[26] In the government politics model, the actions of government emerge not necessarily as a solution to a problem but rather as a result from "compromise, conflict, and confusion of officials" with diverse interests flowing from the organizations they represent.[27]

The federal government's long-standing perspective on encryption reflected the strong organizational prerogatives of the NSA and FBI. Early decisions on encryption policy during the 1990s clearly resulted from a decision process dominated by intelligence and law enforcement organizations and reflected their organizational preferences for vigorous export controls and lawful access to encryption keys through

---

[24] The White House, Office of Press Secretary, Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Undersecretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, September 16, 1999; available at <http://www.info-sec.com/crypto99/crypto_092199a_j.shtml>; accessed on November 2, 1999.
[25] Graham T. Allison and Phillip D. Zelikow, *Essence of Decision*, 2d ed. (New York: Addison-Wesley Educational Publishing, 1999), 143.
[26] Ibid, 150-151.
[27] Ibid, 294-295.

key recovery or key escrow. In essence, the FBI and NSA desired to protect their special capacities to intercept or collect communications and information of foreign governments, criminals, and terrorists. Driven by law enforcement and national security concerns, the implied goal of the various Administration's encryption proposals was to guarantee government access to encrypted communications and stored data.[28] Believing that it could not leave encryption development to market forces alone, but realizing government restrictions on domestic use were politically unacceptable, the federal government attempted to indirectly control the domestic encryption market through its export policies.[29] The Clinton Administration "...sought to influence what type of products are available domestically by limiting exports, knowing that companies do not want to make one product for domestic use and one for export."[30] In fact, to many observers it appeared that export controls were "designed to provide leverage for the federal government to foist key recovery on an unwilling market."[31] The Administration repeatedly challenged any rising Congressional legislation that jeopardized the export control policy with classified briefings to vehemently argue national security concerns.[32] Organizational tendencies also proved extremely difficult to overcome. NSA pundits claim, despite their own internal studies on the issue, that the leadership of the NSA failed to realize the use of encryption would expand regardless of government controls

---

[28] Center for Democracy & Technology, "An Overview of Clinton Administration Encryption Policy Initiatives," available at <http://www.cdt.org/crypto/admin /initiatives.shtml>; accessed on November 27, 1999.

[29] Elizabeth Corcoran, "Who Will Hold the Key? Two Bills Reflect the Split Over Restrictions." *The Washington Post*, August 4, 1997; available at <http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/issues.htm>; accessed on December 7, 1999.

[30] Marcia S. Smith and Jane Bortnick Griffith, "Internet: An Overview of Six Key Policy Issues Affecting Its Use and Growth," Congressional Research Service Report 98-67 STM, May 8, 1998, 3-4.

[31] Reinhold, *Strong Cryptography: The Global Tide of Change*, 4.

[32] Jason Fry and Megan Doscher, "Encryption Wars are History," *Dow Jones News*, September 17, 1999; available at <http://www.info-sec.com/crypto99/crypto_ 092199b_j.shtml>, accessed on November 2, 1999.

and that they should focus instead on preparing to operate in a world of widespread encryption.[33] For most of the 1990s the Clinton Administration pursued a tainted view of balance—a view dictated by the perceived needs of the NSA and FBI.

However, balance in this manner proved nearly impossible to attain. Since March of 1998 the Administration actively pursued a dialogue with industry, law enforcement, and privacy groups to find "…ways to make our policy consistent with both market realities and national security and law enforcement concerns."[34] The government politics model of decision making described by Allison and Zelikow suggests the concept of governmental bargaining to reach a decision.[35] An aspect of this model is clearly evident in that the Clinton Administration's latest proposal to relax export restrictions includes specific measures to bolster law enforcement capacities to circumvent or workaround encryption technology, including $80 million for a technical center, as a bargaining chip to garner FBI's concurrence.[36]

Besides a belated recognition of the obvious and a broader attempt at dialogue with the private sector, the larger political calculus may have finally forced a change in policy. The failure to get foreign governments onboard, growing political support for legislation, recent court rulings, and an upcoming election all likely combined to encourage change.

The Clinton Administration proved unable to generate a vital international consensus around controls on strong encryption and provisions for key recovery. In

---

[33] Seymour M. Hersh, "The Intelligence Gap," *The New Yorker* (December 6, 1999); available at <http://cryptome.org/nsa-hersh.htm>; accessed on December 7, 1999.
[34] William Reinsch, Testimony before the U.S. House of Representatives Judiciary Subcommittee on Courts and Intellectual Property, March 4, 1999.
[35] Allison and Zelikow, *Essence of Decision*, 255.
[36] John Simons, "U.S. to Relax Restrictions on Encryption Technology," *The Wall Street Journal*, September 17, 1999. The White House, Office of the Press Secretary, *FACT SHEET: The Cyberspace Electronic Security Act of 1999*, September 16, 1999; available at <http://www.cdt.org/crypto/CESA/CESArevfactsheet2.shtml>; accessed on November 25, 1999.

recognition of the globalization of encryption technology, the Administration saw the importance of establishing an international pattern of encryption control in order for its own encryption policies to succeed.[37] Additionally, the Administration hoped that if encryption controls were accepted by international community, then Congress would find it hard argue in favor of relaxation of export controls.[38] With this mind, the Clinton Administration intensely lobbied other countries, appointed a roving "crypto czar" tasked with bringing foreign countries on board, and specifically directed its international advocacy efforts at the Organization for Economic Cooperation and Development (OECD) in the absence of other international forums.[39] Despite these efforts, the attempt to persuade foreign governments to implement tighter encryption controls failed. For example, the leadership of the European Union has consistently spoke out in favor of allowing the marketplace to guide encryption decisions.[40] France, the only Western government to pass a law outlawing strong encryption without key escrow, rescinded its policy in January 1999.[41] In March of 1999 UK rejected key recovery as ineffective and inconsistent with its national e-commerce desires and in June Germany also rejected the idea of placing restrictions on strong encryption.[42] Not only have foreign governments proven increasingly unwilling to adopt US export control and key recovery policies, they have moved clearly in the opposite direction, toward liberalization.[43]

---

[37] Elinor Mills, "Consensus Needed for Encryption Export Policy to Succeed," *San Francisco Sun*, February 11, 1997; available at <http://www.sunworld.com/sunworldonline/ swol-02-1997/swol-02-encryption.html>; accessed on November 30, 1999.
[38] Solveig Berstein, "The U.S. Government's Encryption Policy Dodge," Cato Institute, September 11, 1996; available at <http://www.cato.org/dailys/9-11-96.html>; accessed on December 7, 1999.
[39] Mills, "Consensus Needed for Encryption Export Policy to Succeed."
[40] Singleton, *Encryption Policy for the 21st Century*, 19.
[41] Cukier, "Scrambled Codes," 228.
[42] Keith Aoki, *Learning Law in Cyberspace: Privacy and Encryption Export Controls,* updated September 26, 1999, 3; available at <http://www.cyberspacelaw.org/aoki>; accessed on December 1, 1999.
[43] Center for Democracy and Technology, "An Overview of Clinton Administration Encryption Policy Initiatives."

The weight of evidence was reinforced by a growing number of independent commissions and studies that had come out in favor of relaxing encryption controls. Table 2 identifies the key commissions and studies. A looming contradiction in federal government policies also appeared. While export controls restricted the domestic use of encryption, another government initiative to protect critical national infrastructures, Presidential Decision Directive-63, implied a wider use of robust encryption in the private sector.[44] Encryption was also seen as a powerful weapon against oppression worldwide that could aid struggling democratic movements to survive and flourish.[45]

TABLE 2. INDEPENDENT STUDIES ON ENCRYPTION EXPORT CONTROLS

STUDY GROUP/REPORT	CONCLUSIONS
National Research Council, Computer Science and Telecommunications Board, *Cryptography's Role in Securing the Information Society* (CRISIS), 1996	- US cryptography policy inadequate to support information security requirements - Key recovery unproven technology - Government should experiment with escrowed encryption for internal use before wider deployment - Benefits of expanded encryption exceed costs - Overall national interests best served by a rational transition to broader use of encryption and a gradual relaxation, but not elimination of export controls
Global Organized Crime Project, *Cybercrime, Cyberterrorism, and Cyberwarfare*, 1998	- Anticipate the widespread use of strong encryption - Stakeholders must negotiate compromise to export control and key management issues - Law enforcement and intelligence must revise traditional sources and means to cope with spread of strong encryption
President's Export Council Subcommitee on Encryption, *Liberalization 2000: Recommendations for Revising the Encryption Export Regulations*	- Create a license free zone by eliminating export controls for products sent to countries that pose no national security concerns - Allow export of encryption to on-line merchants - Allow export of mass market encryption up to key lengths of 128-bits
National Research Council, *Trust in Cyberspace*, 1999	- Widespread use of cryptography inhibited by public policy controversy - Increased use of cryptography crucial to protect the Internet and its end-points - Federal controls on technology losing effectiveness

If this weren't enough, the Administration also faced a growing and determined political opposition in Congress. The two primary encryption export relief bills, the

---

[44] President's Export Council Subcommitee on Encryption, *Liberalization 2000: Recommendations for Revising the Encryption Export Regulations*; available at <http://www.cs.georgetown.edu/~denning/crypto/lib2000.html>; accessed on November 27, 1999.

[45] Singleton, *Encryption Policy for the 21st Century*, 7-9.

Security and Freedom Through Encryption (SAFE) Act H.R. 850 and Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act S.798, faced less forceful opposition in 1999 than their predecessors had in previous legislative seasons.[46] Table 3 compares the key features of these two bills. During 1999 the SAFE Act attracted more than half the House's members as co-sponsors, survived the usual Administration attempts using a national security punch to derail it, and had passed through all five required committees and on its way to the floor of the House.[47]

TABLE 3. 1999 CONGRESSIONAL LEGISLATION ON ENCRYPTION EXPORT RELIEF

LEGISLATION	KEY FEATURES
Security and Freedom Through Encryption Act (SAFE) H.R. 850	- Americans free to use and sell encryption domestically - Allows export of strong encryption products after a one-time technical review - Maintains controls on encryption exports to hostile nations
Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) S. 798	- Americans free to use and sell encryption domestically - Decontrols export of strong encryption products if items are already available from foreign suppliers - Creates Export Advisory Board to determine which products are available from foreign providers - Requires removal of export controls on strong encryption once the next generation of the American Encryption Standard is released in 2002

Source: "Reforming Encryption Export Controls," The Democratic Leadership Council Briefing, May 24, 1999; available at <http://www.dlcppi.org/briefing/b990524.htm>; accessed on November 30, 1999.

Behind the growing opposition in Congress to encryption export controls sits private advocacy organizations representing the interests of business and civil libertarians. Some of these groups and their primary orientation are listed in Table 4. Although civil libertarian groups played a key role in raising the issue in the public spectrum and communicating information to the public and interested parties, commercial pressures and business interest groups have been much more successful in

[46] "Reforming Encryption Export Controls," The Democratic Leadership Council Briefing, May 24, 1999; available at <http://www.dlcppi.org/briefing/b990524.htm>; accessed on November 30, 1999.
[47] Fry and Doscher, "Encryption Wars are History."

pressuring the Administration and Congress.[48] Even after the latest policy announcement by the Administration in September 1999, the business sector teamed with top House Republicans to wage a "fierce lobbying campaign to pass a law relaxing export controls."[49] High-tech lobbyists continuing the battle for legislation against export controls "found no shortage of lawmakers eager to offer a solution."[50]

TABLE 4. PRIVATE ORGANIZATIONS INVOLVED IN ENCRYPTION DEBATE

BUSINESS GROUPS	CIVIL LIBERTY GROUPS
Americans for Computer Privacy	Center for Democracy and Technology
Alliance for Network Security	Electronic Privacy Information Center
Business Software Alliance	Cato Institute
Software Publishers Association	Internet Privacy Coalition
Software and Information Industry Alliance	Cypherpunks
Information Technology Association of America	Project on Gov Secrecy, Federation of Am Scientists
Electronic Frontier Foundation	
Computer Systems Policy Project	
Information Technology Information Council	

The Administration also faced opposition to its policies in the courts. In response to a case involving the release of encryption source code for academic discussions the US Ninth District Court ruled export restrictions on encryption unconstitutional since they constitute a prior restraint in violation of the First Amendment. In its decision summary the District Court argued that the "Supreme Court has treated licensing schemes that act as prior restraints on speech with suspicion because such restraints run the twin risks of encouraging self-censorship and concealing illegitimate abuses of censorial power."[51]

A final factor in the Administration's political calculus leading to the policy shift appears evident in posturing for the upcoming Presidential election involving Vice

---

[48] Karlin Lillington, "Encryption One Element in Security Picture," *Irish Times*, January 29, 1999; available at <http://www.info-sec.com/crypto/99/crypto_020699c_j.shtml>; accessed on November 2, 1999.

[49] "Encryption Regulations Fall Short," *Wired News*, November 24, 1999; available at <http://www.wired.com/news/politics/0,1283,32732,00.html>; accessed on November 25, 1999.

[50] John Simons, "Industry Say Proposal for Selling Data-Scramblers is Now Muddled," *The Wall Street Journal*, November 15, 1999.

[51] U.S. Court of Appeals for the Ninth Circuit, *Bernstein vs US Department of Justice*, 8.

President Al Gore. The relaxation of export controls on encryption eliminated a contentious issue that Republicans could have employed against the Democrats, especially among potential political contributors in high-tech Silicon Valley. Despite his high-tech visions, Al Gore's success with political campaign fund raising in Silicon Valley had fallen behind that of rivals Bill Bradley and George W. Bush. This decision, and more importantly, his leadership role in resolving this issue, clearly placed Al Gore squarely in synch with the high-tech community and offered the potential to make a noticeable difference in his efforts to court favor with Silicon Valley.[52]

An even more cynical interpretation of events surrounding encryption export policy holds that the federal government's intent in its incremental policy changes, each falling short of a full relaxation of controls, was a delaying tactic meant to slow the proliferation of strong encryption and to keep the genie in the bottle just a bit longer—in which case they succeeded.[53]

POLICY-MAKING IN THE INFORMATION AGE

The controversial debate over encryption export policies may signify the emergence of a succession of complex and contentious information related issues confronting policy makers early in the 21st Century. The encryption issue posed an unprecedented dilemma due to the strongly divergent interests of government agencies and the private sector. Yet, the lack of boundaries in cyberspace, the feverish pace of developments in information technology, the central nature of information in the global economy, and the unique

---

[52] Fry and Doscher, "Encryption Wars are History." Ted Bridis, "Clinton-Encryption," Associated Press, September 17, 1999; available at <http://www.info-sec.com/crypto99/crypto_ 092199c_j.shtml>, accessed on November 2, 1999.

[53] George A. Keyworth II, Testimony at the Hearings on Encryption before the U.S. House of Representatives Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection, September 4, 1997, 10; Available at <http://www.pff.org/ congtest/ct090497.html>; accessed on December 7, 1999.

complexities of cyberspace security will surely generate future controversies with similarly perplexing complications.

The convergence of the vigorously debated US encryption export policy at a balance point illustrates the value of a Constitutionally-established framework that pits an executive branch, with its mission oriented departments and agencies, against a legislature, where both operate subject to the oversight and influence of private sector interest groups. Satisfactory resolution of the encryption export policy controversy required substantial involvement of, input from, and interaction with the private sector, even if at times the federal government appeared uninterested or unwilling to actively engage in a dialogue. The public forum for discussing policy alternatives allows sufficient opportunities for actors, both inside and outside government, with competing interests to be heard. As seen with the encryption policy debate, such a forum permits and even encourages an incremental approach to policy making that eventually stumbles to a point that balances competing interests, at least sufficiently to quell the debate.

Despite this apparent Constitutional success, the current government policy-making paradigm defies the realities of the Information Age. If unchanged, shortcomings in this process will certainly confound the ability of future administrations to successfully resolve complex issues involving cyberspace. Taking seven years and an equal number of policy proposals to reach a consensus on a critical issue will prove unacceptable in the fast-paced global environment of the 21st Century. The policy process must evolve to reach faster consensus. The market despises uncertainty and government policy should seek to quickly reduce uncertainty surrounding an issue. Failure to recognize the entire spectrum of an information age issue unnecessarily extends the duration of the resolution

process. Since cyberspace has no borders, policy makers must fully investigate and take into account the global and private sector dynamic surrounding public policy information technology issues. Even more frustrating to policy makers, government initiatives to guide or shape technological development will face nearly insurmountable obstacles. Technology can change faster than technology and "governments can no longer dictate the pace and scope of technological innovation."[54] This limitation looms especially true in the information security arena where federal mandates, controls, and influence grow increasingly less effective due to a greater number of vendors, the lack of a dominant federal market share, the priority of market responsiveness over government cooperation, and an expanding population of foreign vendors and service suppliers. Policy makers must recognize that "…outside certain safety- and reliability-critical contexts, government mandates and controls on technology are decreasingly effective and that some form of cooperation is the logical alternative."[55] In essence, today's policy-making paradigm suffers from an inability to react at speeds demanded by cyberspace issues, an overly narrow perspective of policy problems, and a government-centric solution set. Government must evaluate and transforms its old paradigms and practices to meet the challenges of the new millenium.

An Information Age policy-making paradigm should provide increased public debate on national and international information topics, greater use of public-private partnerships that effectively leverages private sector expertise and input, and a government policy process that incorporates principles of a learning, self-adapting organization. The certain complexity of future information issues and the inherent

---

[54] Ibid, 4.
[55] Schneider, *Trust in Cyberspace*, 219-221.

difficulty of resolving cyberspace issues without understanding the larger national security and economic context demand a larger public discourse. Vigorous discussion over national information priorities and strategies may produce guiding principles that could help unify government policies and build consensus, or at the very least, aid the public and national leadership in understanding the full nature of the issues. Sincere and open dialogue with the private sector must emerge as a central operating premise of government. Issues in cyberspace demand private sector expertise and deliberated viewpoints. In many instances, the government will have no choice but to turn to public-private partnerships to solve urgent problems, the success of which will "depend upon developing increased trust between the private and public sectors, and in particular, the degree of trust in government."[56] Meaningful and productive relationships with the private sector will remain elusive if government unilaterally insists on "…its position or its preferred solutions—even if cloaked in the guise of promoting partnerships with or education of non-governmental entities…."[57] However, perfecting a governing style based on dialogue with the private sector remains an intimidating challenge. Unlike the encryption debate where business and civil libertarian groups took the same side, future issues may see the private sector divided into divergent and conflicting camps making a consensus reaching dialogue with the private sector more difficult. The transformation of government into a more adaptive policy making body, capable of quickly learning from past mistakes, suggests an engaging goal, albeit probably illusive. The *first lesson*: both the government and private sector must understand that the encryption export policy controversy stands as an example of a policy that failed due to shortcomings in a process

[56] Ibid, 219.
[57] Ibid, 219-220.

ill-suited or ill-focused for an effective discourse on cyberspace issues. Stakeholders must make the effort to thoroughly review the process history behind this issue to more fully understand the process failure modes and potential process alternatives in this case. Public-private partnerships and dialogues that work must be expanded, reinforced, and duplicated where appropriate. America has no time to waste—the next controversial issue already transits our information networks.

The value of a decision making process is found in the quality of the decisions produced by the process. The Information Age will certainly challenge our national decision making process. The encryption export policy debate suggested several aspects of the Information Age that will confound policy makers in the 21st Century. Old government paradigms and practices must not follow the nation into the new millenium. Government must fuse itself closer to the private sector, not just to meet business interests but to respond to the concerns of individuals living, working, and existing in cyberspace. America's children can already use Information Age tools better than their parents. America's leaders should respond to this enthusiasm by forging a new national decision making process that can successfully balance the benefits and risks of cyberspace.

BIBLIOGRAPHY

Allison, Graham T. and Phillip D. Zelikow. *Essence of Decision*, 2d ed. New York: Addison-Wesley Educational Publishing, 1999.

Aoki, Keith. *Learning Law in Cyberspace: Privacy and Encryption Export Controls.* Updated September 26, 1999. Available at <http://www.cyberspacelaw.org/aoki>; accessed on December 1, 1999.

Bernstein, Solveig. "The U.S. Government's Encryption Policy Dodge." Cato Institute, September 11, 1996. Available at <http://www.cato.org/dailys/9-11-96.html>; accessed on December 7, 1999.

Bridis, Ted. "Clinton – Encryption." Associated Press, September 17, 1999. Available at <http://www.info-sec.com/crypto99/crypto_ 092199c_j.shtml>; accessed on November 2, 1999.

Center for Democracy & Technology. "An Overview of Clinton Administration Encryption Policy Initiatives." Available at <http://www.cdt.org/crypto/admin /initiatives.shtml>; accessed on November 27, 1999.

Corcoran, Elizabeth. "Who Will Hold the Key? Two Bills Reflect the Split Over Restrictions." The Washington Post, August 4, 1997. Available at <http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/issues.htm>; accessed on December 7, 1999.

Cukier, Kenneth N. "Scambled Codes." *Red Herring* (December 1999), 227-234.

Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo. By William H. Webster, Chairman, Global Organized Crime Project. Washington D.C.: Center for Strategic and International Studies, 1998.

Dam, Kenneth W. and Herbert S. Lin. "Protecting Information in Cyberspace." National Academy Op-Ed Service, September 13, 1966. Available at <http://www4.national academies.org>; accessed on December 7, 1999.

"Encryption Regulations Fall Short." *Wired News*, November 24, 1999. Available at <http://www.wired.com/news/politics/0,1283,32732,00.html>; accessed on November 25, 1999.

Fry, Jason and Megan Doscher. "Encryption Wars are History." *Dow Jones News*, September 17, 1999. Available at <http://www.info-sec.com/crypto99/crypto_ 092199b_j.shtml>; accessed on November 2, 1999.

Hersh, Seymour M. "The Intelligence Gap." *The New Yorker* (December 6, 1999), 58-76. Available at <http://cryptome.org/nsa-hersh.htm>; accessed on December 7, 1999.

Keyworth, George A. II. Testimony at the Hearings on Encryption before the U.S. House of Representatives Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection. September 4, 1997. Available at <http://www.pff.org/congtest/ct090497.html>; accessed on December 7, 1999.

Lillington, Karlin. "Encryption One Element In Security Picture." *Irish Times*, January 29, 1999. Available at <http://www.info-sec.com/crypto/99/crypto_020699c_j.shtml>; accessed on November 2, 1999.

McNamara, Barbara. Testimony before the U.S. House of Representatives Judiciary Subcommittee on Courts and Intellectual Property. March 4, 1999. Available at <http://www.usia.gov/current/news/ latest/99030402.clt.html?/products/washfile/newsitem.shtml>.

Mills, Elinor. "Consensus needed for encryption export policy to succeed." *San Francisco Sun*, February 11, 1997. Available at <http://www.sunworld.com/sunworldonline/swol-02-1997/swol-02-encryption.html>; accessed on November 30, 1999.

O'Harrow, Robert, Jr. "Agency Says Encryption Law Needed." *The Washington Post*, August 21, 1999.

President's Export Council Subcommittee on Encryption. *Liberalization 2000: Recommendations for Revising the Encryption Export Regulations*. Available at <http://www.cs.georgetown.edu/~denning/crypto/lib2000.html>; accessed on November 27, 1999.

"Reforming Encryption Export Controls." The Democratic Leadership Council Briefing, May 24, 1999. Available at <http://www.dlcppi.org/briefing/b990524.htm>; accessed on November 30, 1999.

Reinhold, Arnold G. *Strong Cryptography: The Global Tide of Change*. Cato Institute Briefing Paper No. 51. September 17, 1999. Available at <http://www.cato.org>.

Reinsch, William. Testimony before the U.S. House of Representatives Judiciary Subcommittee on Courts and Intellectual Property. March 4, 1999.

Schneider, Fred B., ed. *Trust in Cyberspace*. Washington D.C.: National Academy Press, 1999.

Simons, John. "U.S. to Relax Restrictions on Encryption Technology." *The Wall Street Journal*, September 17, 1999.

Simons, John. "Industry Say Proposal for Selling Data-Scramblers is Now Muddled." *The Wall Street Journal*, November 15, 1999.

Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. New York: Doubleday, 1999.

Singleton, Solveig. *Encryption Policy for the 21st Century: A Future Without Government-Prescribed Key Recovery*. Cato Institute Policy Analysis No. 325, November 19, 1998.

Smith, Marcia S. and Jane Bortnick Griffith. "Internet: An Overview of Six Key Policy Issues Affecting Its Use and Growth." Congressional Research Service Report 98-67 STM. May 8, 1998.

The White House. Office of Press Secretary. Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Undersecretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, September 16, 1999. Available at <http://www.info-sec.com/crypto99/crypto_092199a_j.shtml>; accessed on November 2, 1999.

The White House. Office of Press Secretary. *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace*. William Cohen, Janet Reno, Jacob J. Lew, and William Daley. Released September 16, 1999. Available at <http://www.epic.org/crypto/legislation/cesa/report_9_16_.html>; accessed on November 8, 1999.

The White House. Office of the Press Secretary. *FACT SHEET: The Cyberspace Electronic Security Act of 1999*. Released September 16, 1999. Available at <http://www.cdt.org/crypto/CESA/ CESArevfactsheet2.shtml>; accessed on November 25, 1999.

United States Court of Appeals for the Ninth Circuit. *Bernstein vs US Department of Justice*. Case Number: 97-16686, filed May 6, 1999. Available at <http://www.epic.org/crypto/export_controls/bernstein_decision_9_cir.html>; accessed on November 27, 1999.

Winston, Joan D., Kenneth A. Mendelson, and Stephen T. Walker. "Light at the End of the Tunnel? Finding a Way Through the Crypto Policy Impasse." (151-165) In *Cyberwar 2.0: Myths, Mysteries and Reality* eds Alan D. Campen and Douglas H. Dearth. Fairfax: AFCEA International Press, 1998.